

FortiClient (Windows) - Release Notes

VERSION 5.2.6

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



July 10, 2017

FortiClient (Windows) 5.2.6 Release Notes

04-526-381033-20170710

TABLE OF CONTENTS

Change Log	4
Introduction	5
Licensing	5
Client limits	5
Special Notices	7
SSL VPN on Windows 10	7
Using FortiClient VPN with other Third-Party VPN Clients	7
Conflicts with Cisco Systems VPN Client	7
FortiClient registration database synchronization	7
Installing on Windows 7, Windows XP, and Windows Server 2008 R2	8
Installation Information	9
Firmware images and tools	9
Upgrading from previous FortiClient versions	9
Downgrading to previous versions	9
Firmware image checksums	10
Product Integration and Support	11
FortiClient 5.2.6 support	11
Language support	12
Conflicts with third party antivirus products	13
Conflicts with Cloud App Discovery	13
Resolved Issues	14
Known Issues	15

Change Log

Date	Change Description
2016-07-22	Initial release.
2017-07-10	Updated to clarify support for FortiOS 5.4.0 and later.

Introduction

This document provides a summary of enhancements, support information, and installation instruction for FortiClient (Windows) 5.2.6 build 0664. Please review all sections prior to installing FortiClient.

- [Introduction](#)
- [Special Notices](#)
- [Installation Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Installation Information](#)

Please review all sections prior to installing FortiClient.

Licensing

Licensing on the FortiGate is based on the number of registered clients. FortiGate 30 series and higher models support ten (10) free managed FortiClient licenses. For additional managed clients, a FortiClient license subscription must be purchased. The maximum number of managed clients varies per device model.

Client limits

The following table shows client limits per FortiGate model series.

The ability to download the license file, pre-configure the client, create a custom installer, and rebrand are included.

FortiClient license upgrade

FortiGate Series	Free Registrations	FortiClient License Upgrade
FortiGate/FortiWiFi 30 to 90 series	10	1 year FortiClient license subscription for up to 200 clients
FortiGate 100 to 300 series	10	1 year FortiClient license subscription for up to 600 clients
FortiGate 500 Series & above FortiGate VM01 /w FOS 5.4 & above	10	1 year FortiClient license subscription for up to 2000 clients
FortiGate 1000 series & above FortiGate VM04 /w FOS 5.4 & above	10	1 year FortiClient license subscription for up to 8000 clients
FortiGate 3000 series & above FortiGate VM08 /w FOS 5.4 & above	10	1 year FortiClient license subscription for up to 20 000 clients



In high availability (HA) configurations, all cluster members require an upgrade license key.

Special Notices

SSL VPN on Windows 10

When a custom DNS server is configured for SSL VPN, sometimes Windows 10 DNS resolution is not correct after the SSL VPN is connected.

The following FortiClient XML configuration is recommended, so that FortiClient restarts Windows dnscache service when SSL is connected.

```
<sslvpn>
  <options>
    <dnscache_service_control>2</dnscache_service_control>
  </options>
</sslvpn>
```

Using FortiClient VPN with other Third-Party VPN Clients

It is not supported to run more than one VPN connection simultaneously. If using any third-party VPN software (other than FortiClient), please disconnect FortiClient VPN first, before establishing connection with the other VPN software. To reconnect VPN using FortiClient, ensure to first disconnect any established VPN connection from a third-party VPN software.

Conflicts with Cisco Systems VPN Client

FortiClient VPN feature conflicts with Cisco Systems VPN Client 5.0.07.

When both Cisco VPN Client 5.0.07 and FortiClient VPN are installed on the same Windows computer, a BSOD is likely to occur if an IPsec VPN connection is established using FortiClient.

Cisco VPN Client 5.0.07 has reached end of support. It is suggested to use Cisco AnyConnect 3.1 or newer instead. This is actively maintained by Cisco Systems. With Cisco Anyconnect installed, a BSOD does not occur when using FortiClient to establish an IPsec VPN connection.

Please note that it is unknown what may occur if VPN connections are attempted using both Cisco Anyconnect and FortiClient VPN at the same time. This is not recommended. Consider disconnecting one VPN connection, before establishing a second one.

FortiClient registration database synchronization

FortiGate is not able to synchronize its FortiClient registration database between 32-bit and 64-bit platforms.

Installing on Windows 7, Windows XP, and Windows Server 2008 R2

FortiClient 5.2.6 files and drivers are digitally signed using SHA2 certificates. Microsoft Windows 7 and Windows XP are both known to have issues with the verification of SHA2 certificates. Ensure you have the update installed described in the *Affected Software* section of the Advisory for your operating system from the following link:

[Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2](#)

Installation Information

Firmware images and tools

When installing FortiClient version 5.2.6, you can choose the setup type that best suits your needs. You can select one of the two options: Complete: All Endpoint Security and VPN components will be installed or VPN Only: only VPN components (IPsec and SSL) will be installed.

- FortiClientSetup_5.2.6.0664.exe

Standard installer for Microsoft Windows (32-bit).

- FortiClientSetup_5.2.6.0664.zip

A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.

- FortiClientSetup_5.2.6.0664_x64.exe

Standard installer for Microsoft Windows (64-bit).

- FortiClientSetup_5.2.6.0664_x64.zip

A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.

- FortiClientTools_5.2.6.0664.zip

A zip package containing miscellaneous tools including the FortiClient Configurator tool and VPN Automation files.



When creating a custom FortiClient 5.2.6 installer using the FortiClient Configurator tool, you can choose which features to install. You can enable or disable software updates, configure SSO, and rebrand FortiClient .

Upgrading from previous FortiClient versions

FortiClient version 5.2.6 supports upgrade from FortiClient version 5.0.9 and later.

Downgrading to previous versions

Downgrading FortiClient version 5.2.6 to previous FortiClient versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at <https://support.fortinet.com>. After logging in, click on *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 5.2.6 support

The following table lists version 5.2.6 product integration and support information.

FortiClient 5.2.6 support information

Desktop Operating Systems	<ul style="list-style-type: none">• Microsoft Windows XP (32-bit)• Microsoft Windows 7 (32-bit and 64-bit)• Microsoft Windows 8 (32-bit and 64-bit)• Microsoft Windows 8.1 (32-bit and 64-bit)• Microsoft Windows 10 (32-bit and 64-bit)
Server Operating Systems	<ul style="list-style-type: none">• Microsoft Windows Server 2008 R2• Microsoft Windows Server 2012, 2012 R2
Minimum System Requirements	<ul style="list-style-type: none">• Microsoft Internet Explorer version 8 or later• Microsoft Windows compatible computer with Intel processor or equivalent• Compatible operating system and minimum 512MB RAM• 600MB free hard disk space• Native Microsoft TCP/IP communication protocol• Native Microsoft PPP dialer for dial-up connections• Ethernet network interface controller (NIC) for network connections• Wireless adapter for wireless network connections• Adobe Acrobat Reader for FortiClient documentation• Windows Installer MSI installer version 3.0 or later.
FortiAnalyzer	<ul style="list-style-type: none">• 5.0.2 and later• 5.2.0 and later• 5.4.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 2.2.0 and later• 3.0.0 and later• 3.1.0 and later• 3.2.0 and later
FortiManager	<ul style="list-style-type: none">• 5.0.2 and later• 5.2.0 and later• 5.4.0 and later

FortiOS

- 5.0.0 and later
- 5.2.0 and later
- 5.4.0

FortiClient IPsec VPN and SSL VPN support FortiOS 5.4.0 and later.

Some FortiClient features are dependent on specific FortiOS versions.

Language support

The following table lists FortiClient language support information.

FortiClient language support

Language	Graphical User Interface	XML Configuration	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓		
Chinese (Traditional)	✓		
French (France)	✓		
German	✓		
Japanese	✓		
Korean	✓		
Portuguese (Brazil)	✓		
Russian	✓		
Spanish (Spain)	✓		

The FortiClient language setting defaults to the regional language setting configured on the client workstation unless configured in the XML configuration file.



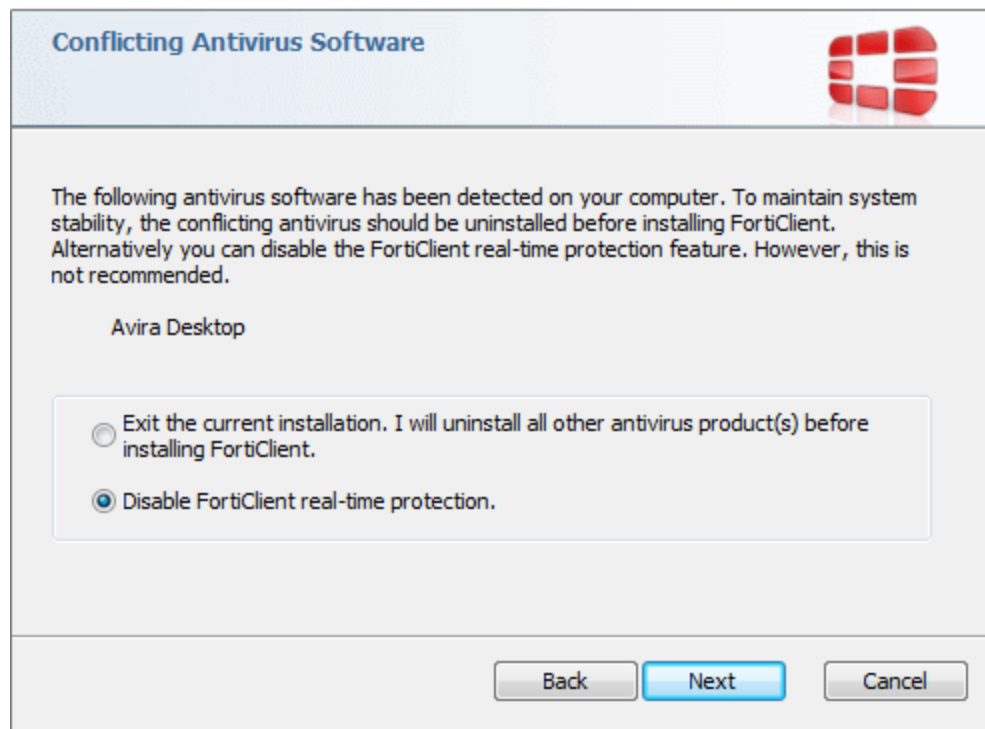
If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market. Consider removing other antivirus programs before installing FortiClient.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).

Conflicting Antivirus Software



Conflicts with Cloud App Discovery

When enabled, FortiClient Web Filtering displays a replacement message in web browsers if a web page is blocked. The replacement message is displayed for both HTTP and HTTPS traffic.

With the new [Microsoft Cloud App Discovery](#) installed, FortiClient Web Filter replacement message will not be displayed for HTTP sites. They seem to be suppressed by the Cloud App Discovery process. The HTTP web sites are blocked appropriately, as evident by FortiClient log entries. Replacement messages for HTTPS sites will still display correctly.

Resolved Issues

The following issues have been fixed in version 5.2.6. To report any issues, please contact [Customer Service & Support](#).

AntiVirus

Bug ID	Description
0289962	SSL VPN cross VDOM script execution of <i>on connect</i> script.
0310102	After installing FortiClient, Adobe Acrobat considers that assistive technology is used.

VPN

Bug ID	Description
0372313	FortiClient PKI IPsec VPN cannot connect from command line during SCCM deployment.
0376438	Traffic isn't sent via IPsec when both wired and WiFi connections are available.
0368718	FortiClient IPsec tunnel is shut down once endpoint profile is pushed to clients.
0304679	VPN before Windows logon prompts for certificate when it should not.

Web Filter

Bug ID	Description
0308591	FortiClient is causing high delay for Microsoft Direct Access traffic.

Other

Bug ID	Description
0281556	OpenSSL Security Advisory [11 Jun 2015]

Known Issues

The following issues have been identified in FortiClient (Windows) 5.2.6. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
0294877	FortiClient SSLVPN may not be able to add route when CISCO AnyConnect VPN is also connected.



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.